

REMARKS

This Application has been carefully reviewed in light of the *Office Action* and an *Advisory Action* dated May 19, 2009 (the “*Advisory Action*”). At the time of the *Advisory Action*, Claims 1-26 and 30-34 were pending and rejected. Applicant has amended Claims 1, 4, 9, 16, and 34 and added Claim 35. Applicant respectfully requests reconsideration and favorable action in this case in view of the following remarks.

Rejections Under 35 U.S.C. § 101

The Examiner rejected Claims 9-15, 25, 28 and 31 under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter. While Applicant does not necessarily agree with the propriety of this rejection, and solely to advance prosecution, Applicant has amended Claim 9 to include “a tangible processor controlled device comprising a reverse proxy server.” Accordingly, Applicant respectfully requests the Examiner to withdraw the rejections of Claims 9-15, 25, 28 and 31 under 35 U.S.C. § 101.

Rejections Under 35 U.S.C. § 102 and §103

The Examiner rejected Claims 1-5, 9-11, 15-20, 24-32 and 34 under 35 U.S.C. § 102(b) as allegedly being anticipated by U.S. Publication No. 2003/0061515 to Kindberg et al. (“*Kindberg*”). The Examiner rejected Claims 6-8, 12-14, and 21-23 under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Kindberg* in view of U.S. Patent No. 7,080,000 to Cambridge (“*Cambridge*”). The Examiner further rejected Claim 33 under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Kindberg* in view of U.S. Patent No. 6,968,394 to El-Rafie (“*El-Rafie*”). Applicant respectfully traverses those rejections for the reasons stated below.

I. *Kindberg* fails to disclose the limitations of amended Claim 1.

Claim 1, as amended, is directed to a method for maintaining computer security. The method includes providing a signature file containing information about known system vulnerabilities, the information including a predefined length of a Universal Resource Locator (“URL”) for a message header. The method further includes, at a reverse proxy server residing between at least one client computer and a web server, receiving an incoming message from the at least one client computer. If malicious, the incoming message

automatically causes the web server to perform an action which exploits a vulnerability of the web server upon receipt by the web server. To determine whether the incoming message is malicious, a length of a URL in a message header of the incoming message (“the incoming URL”) is compared with the predefined length in the signature file, and if the length of the incoming URL exceeds the predefined length, the incoming message is determined to be malicious and is blocked from reaching the web server. *Kindberg* fails to disclose, teach or suggest this combination of limitations.

For example, *Kindberg* fails to show “at a reverse proxy server residing between at least one client computer and a web server . . . comparing a length of a URL in a message header of the incoming message (“the incoming URL”) with the predefined length in the signature file . . . [and] . . . if the length of the incoming URL exceeds the predefined length, determining that the incoming message is malicious and blocking the incoming message from reaching the web server.” Rather, *Kindberg* merely discloses “[a] mechanism for providing a user with selective access to resources on an intranet” See *Kindberg*, Abstract. As explained by *Kindberg*, “[c]apabilities are used to represent URLs of resources within the domain 200. In order to use a capability, a client 203 must present the capability to a reverse proxy server 201 running on the firewall of the domain 200 Upon receiving a capability-enabled URL, the reverse proxy server verifies its authenticity and then issues a request to the intranet web server 202 which manages the resource.” See *Kindberg*, paragraphs [0035] - [0037] (emphasis added). Furthermore, *Kindberg* discloses that:

[A] capability character string **may be recognized as such** by referring to the table used to track issued capabilities and avoid capability/URL ambiguity. Alternatively, all URLs having a character string conforming to the length and composition conforming to the established capability format (allowing for escape sequences if present) may be passed to step 605.

Kindberg, paragraph [0052] (emphasis added). That is, *Kindberg* merely discloses that a URL may be recognized as being capability-enabled if its character string conforms to the established capability format (i.e., in length and composition). However, *Kindberg* fails to disclose, teach, or suggest “if the length of the incoming URL exceeds the predefined length, determining that the incoming message is malicious and blocking the incoming message from reaching the web server.” as recited in Claim 1.

For at least these reasons, independent Claim 1 and its dependent claims are allowable under 35 U.S.C. § 102 and 35 U.S.C. § 103. For analogous reasons, independent Claims 9, 16, and 34 and their respective dependent claims are allowable under 35 U.S.C. § 102 and 35 U.S.C. § 103.

II. New Claim

Applicant has added new Claim 35 which is fully supported by the Specification as originally filed and add no new matter. Applicant respectfully contends that none of the cited references disclose, or even teach or suggest, either alone or in combination, the combination elements recited in that claim. As one example, Claim 35 depends from an allowable independent claim, as discussed above. As another example, no reference shows that “the predetermined length indicates a maximum amount of data that may be stored in a buffer of the web server before the buffer overflows, the length of the incoming URL indicates an amount of data that the incoming message will attempt to store on the buffer if the incoming message is received by the web server; and the step of determining that the incoming message is malicious comprises determining that the incoming message is capable of causing the buffer to overflow” as recited in Claim 35.

III. All Claims are in condition for allowance.

For at least the reasons stated above, Applicant respectfully contends that each and every claim is in condition for allowance. Moreover, Applicant respectfully contends that none of the deficiencies described above with respect to *Kindberg* are accounted for by any of the remaining references cited by the Examiner or by the knowledge of one of ordinary skill in the art.

IV. No Waiver

Additionally, Applicant has merely discussed example distinctions from the references cited by the Examiner. Other distinctions may exist, and Applicant reserves the right to discuss these additional distinctions in a later Response or on Appeal, if appropriate. By not responding to additional statements made by the Examiner, Applicant does not acquiesce to the Examiner’s additional statements, nor does Applicant necessarily concede to the veracity of any characterization of Applicant’s claims or the prior art references made by

the Examiner. The example distinctions discussed by Applicant are sufficient to overcome the Examiner's rejections.

CONCLUSION

Applicant has made an earnest attempt to place this case in condition for allowance. For at least the foregoing reasons, Applicant respectfully requests full allowance of all pending claims.

If the Examiner feels that a telephone conference would advance prosecution of this Application in any manner, the Examiner is invited to contact the undersigned Attorney for Applicant, at the Examiner's convenience at (214) 953-6655.

The Examiner is requested to charge the Request for Examination fee of **\$810.00** and any additional required fees or credit any overpayments to **Deposit Account No. 02-0384 of Baker Botts L.L.P.**

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicant



Luke K. Pedersen
Reg. No. 45,003

Date: June 1, 2009

CORRESPONDENCE ADDRESS:

Customer No. **05073**